

CLAIMS

What is claimed is:

- 1 1. A computerized method for automatically configuring a firewall comprising:
2 determining a zone for a network address assigned to a network adapter; and
3 associating a security policy for the zone with the network adapter, the security
4 policy specifying the firewall configuration.
- 1 2. The computerized method of claim 1 further comprising:
2 determining the network address assigned to the network adapter.
- 1 3. The computerized method of claim 1, wherein the zone is defined by a set of
2 network addresses.
- 1 4. The computerized method of claim 3, wherein the set of network addresses
2 comprises at least one address within the zone.
- 1 5. The computerized method of claim 3, wherein the set of network address
2 comprises at least one address outside the zone.
- 1 6. The computerized method of claim 1 further comprising:
2 assigning the security policy to the zone.
- 1 7. The computerized method of claim 1 further comprising:
2 retrieving a policy file that contains definitions for the zone and the security policy
3 and specifies that the security policy is assigned to the zone.
- 1 8. The computerized method of claim 7 further comprising:

2 creating the policy file from data input by a user.

1 9. The computerized method of claim 7 further comprising:

2 creating the policy file from data input by an administrator.

1 10. The computerized method of claim 7 further comprising:

2 receiving data from a pre-determined location on a network through the network
3 adapter; and

4 creating the policy file from the data.

1 11. A computer-readable medium having computer-executable instructions
2 comprising:

3 determining a zone for a network address assigned to a network adapter; and
4 associating a security policy for the zone with the network adapter, the security
5 policy specifying the firewall configuration.

1 12. The computer-readable medium of claim 11 having further computer-readable
2 instructions comprising:

3 determining the network address assigned to the network adapter.

1 13. The computer-readable medium of claim 11 having further computer-readable
2 instructions comprising:

3 assigning the security policy to the zone.

1 14. The computer-readable medium of claim 11 having further computer-readable
2 instructions comprising:

3 retrieving a policy file that contains definitions for the zone and the security policy
4 and specifies that the security policy is assigned to the zone.

1 15. The computer-readable medium of claim 14 having further computer-readable
2 instructions comprising:
3 creating the policy file from data input by a user.

1 16. The computer-readable medium of claim 14 having further computer-readable
2 instructions comprising:
3 creating the policy file from data input by an administrator.

1 17. The computer-readable medium of claim 14 having further computer-readable
2 instructions comprising:
3 receiving data from a pre-determined location on a network through the network
4 adapter; and
5 creating the policy file from the data.

1 18. The computer-readable medium of claim 11 having further computer-readable
2 instructions comprising:
3 defining the zone based on a set of network addresses.

1 19. The computer-readable medium of claim 18 having further computer-readable
2 instructions comprising:
3 including at least one address within the zone in the set of network addresses.

1 20. The computer-readable medium of claim 18 having further computer-readable
2 instructions comprising:
3 including at least one address outside the zone in the set of network addresses.

1 21. A computerized system comprising:
2 a processing unit;

3 a memory coupled to the processing unit through bus;
4 a network adapter coupled to the processing unit through the bus and further
5 operable for coupling to a network; and
6 a firewall configuration process executed from the memory by the processing unit
7 to cause the processing unit to determine a zone for a network address assigned to the
8 network adapter and to associate a firewall security policy for the zone with the network
9 adapter.

1 22. The computerized system of claim 21 further comprising a firewall process
2 executed from the memory by the processing unit to cause the processing unit to filter data
3 addressed to the network adapter according to the security policy.

1 23. The computerized system of claim 21 wherein the firewall configuration process is
2 executed by the processing unit when the network address for the network adapter
3 changes.

1 24. The computerized system of claim 21 wherein the firewall configuration process
2 further causes the processing unit to determine the network address of the network adapter.

1 25. The computerized system of claim 21 wherein the firewall configuration process
2 further cause the processing unit to define the zone based on a set of network addresses.

1 26. The computerized system of claim 25, wherein the set of network addresses
2 comprises at least one address within the zone.

1 27. The computerized system of claim 25, wherein the set of network addresses
2 comprises at least one address outside the zone.

1 28. The computerized system of claim 21, wherein the firewall configuration process
2 further cause the processing unit to assign the security policy to the zone.

1 29. The computerized system of claim 21, wherein the firewall configuration process
2 further cause the processing unit to retrieve a policy file that contains definitions for the
3 zone and the security policy and specifies that the security policy is assigned to the zone.

1 30. The computerized system of claim 29, wherein the firewall configuration process
2 further cause the processing unit to receive data from a user and to create the policy file
3 from the data.

1 31. The computerized system of claim 29, wherein the firewall configuration process
2 further cause the processing unit to receive data from an administrator and to create the
3 policy file from the data.

1 32. The computerized system of claim 29, wherein the firewall configuration process
2 further cause the processing unit to receive data from a pre-determined location on a
3 network through the network adapter and to create the policy file from the data.

1 33. A computer-readable medium having stored thereon policy file data structure
2 comprising:

3 a policy identifier field containing data representing an identifier for a security
4 policy;

5 a protocol identifier field containing data representing an identifier for a protocol
6 associated with the security policy identified in the policy identifier field; and

7 a protocol element entry containing data representing a protocol element for the
8 protocol identified by the protocol identifier field.

1 34. The computer-readable medium of claim 33, wherein the protocol element is
2 chosen from the group consisting of ports and services.

1 35. The computer-readable medium of claim 33, wherein the protocol element entry
2 comprises:
3 an element identifier field containing data representing an identifier for the
4 protocol element field; and
5 a settings field containing data representing a filter setting for the protocol element
6 identified by the element identifier field.

1 36. The computer readable medium of claim 35, wherein the filter setting is chosen
2 from the group consisting of allow, disallow, source address and destination address.

1 37. The computer-readable medium of claim 35, wherein the protocol element entry
2 further comprises:
3 a log indicator field containing data representing an decision on logging data
4 utilizing the protocol element identified by the element identifier field.

1 38. The computer-readable medium of claim 33 further comprising:
2 a zone identifier field containing data representing an address zone;
3 an address parameters field containing data representing a set of network addresses
4 that defines the zone identified by the zone identifier field; and
5 an assigned policy identifier containing data representing the identifier for the
6 security zone assigned to the zone identified by the zone identifier field.

1 39. The computer-readable medium of claim 38, wherein the address parameters field
2 contains data representing at least one address within the zone.

